BY ORDER OF THECOMMANDER
AIR MOBILITY COMMAND

AMC INSTRUCTION 14-106

1 JUNE 1999

Intelligence

THREAT WORKING GROUP (TWG)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: A copy of this publication can be found digitally at http: www.safb.af.mil:80/hqamc/pa/pubs/pubhome2.htm. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AMC/INO
(Mr. William E. Chmelir)
Supersedes AMCI 14-106, 24 September 1997

Certified by: HQ AMC/INO
(Lt Col Nicholas M. Turk)
Pages: 34
Distribution: F

This instruction implements AFPD 14-1, Air Force Intelligence Planning and Operations, and prescribes guidelines for the Threat Working Group operating at the headquarters and unit levels. It assigns responsibility for managing the process. This does not apply to Air National Guard or Air Force Reserve Command units.

SUMMARY OF REVISIONS

This revision of the AMCI clarifies functional responsibilities and Threat Working Group processes and membership. Three new attachments **Attachment 3**, **Attachment 5**, and **Attachment 6** have been included that describe the process of maintaining the Phoenix Raven-required list and two operational risk management tools used to assess the threat to specific airfields.

Chapter 1—THREAT WORKING GROUP **3**

1.1. Charter: 3

1.2. Membership: 3

1.3. Processes: 3

1.4. Products: 4

Chapter 2—HEADQUARTERS AMC RESPONSIBILITIES **6**

2.1. Director of Intelligence-(IN): 6

2.2. Director of Security Forces-(SF): 7

2.3. Tanker Airlift Control Center (TACC)-(OPR: TACC/XOZ): 7

2.4. AFOSI Region 3: 8

2.5. USTRANSCOM/J2: 8

2.6. USTRANSCOM Counterintelligence Support Office (CISO): 8

2.7. Director of Central Intelligence Representative (DCI Rep): 8

2.8. National Security Agency Representative (NSA Rep): 9

2.9. Defense Intelligence Agency Representative (DIA Rep): 9

2.10. Counterintelligence Support-Air Force Office of Special Investigations 10

2.11. Director of Operations (DO): 10

2.12. National Reconnaissance Office Representative (NRO Rep): 11

2.13. Air Intelligence Agency (AIA)-Det 4: 11

Chapter 3—WING, DIRECT REPORTING UNIT (DRU), AND GEOGRAPHICALLY SEPARATED UNIT (GSU) LEVEL RESPONSIBILITIES 12

3.1. Requirements 12

3.2. Responsibilities: 12

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 13

Attachment 2—AIR MOBILITY COMMAND'SFORCE PROTECTIONESSENTIAL ELEMENTS OF INFORMATION 17

Attachment 3—PHOENIX RAVEN REQUIRED LIST MAINTENANCE PROCESS 24

Attachment 4—SAMPLE AMC THREAT WORKING GROUP (TWG) AIRFIELD RISK ASSESSMENT 25

Attachment 5—AIRFIELD MANPAD THREAT ASSESSMENT 30

Attachment 6—AMC THREAT WORKING GROUP OPERATIONAL RISK ASSESSMENT 33

Chapter 1

THREAT WORKING GROUP

1.1. Charter:

1.1.1. The AMC Threat Working Group (TWG) provides AMC/CC/CV, the Tanker Airlift Control Center (TACC), and all AMC units with a single focal point for coordinated all-source threat analysis for ongoing and future operations.

1.1.2. Daily TWG meetings combine intelligence, operations, counterintelligence, security, and force protection functions in one comprehensive working group to develop risk assessments and force protection recommendations.

1.2. Membership:

1.2.1. TWG principal membership includes representatives from IN, DO, TACC, SF, AFOSI Region 3, and USTRANSCOM/J2.

1.2.1.1. A principal and/or at least one action officer for each functional area attend the daily TWG meetings.

1.2.1.2. The TWG, in the form of representatives from IN, AFOSI, and SF, is on call to the TACC 24-hours-a-day.

1.2.2. Associate members include representatives from the National Intelligence Agencies (CIA, DIA, NIMA, NSA, and NRO).

1.2.3. Other internal and external AMC organizations support the TWG with products, services, and inputs.

1.2.3.1. The AMC/SG provides the TWG medical-related information that could potentially impact deployed AMC personnel.

1.3. Processes:

1.3.1. The TWG meets to discuss current and potential threats affecting AMC planning and operations, including AMC-contracted commercial carrier missions.

1.3.2. The TWG reviews AMC/INO's Secure Launch Country List from which the TACC derives its Secure Launch List.

1.3.3. AMC/INO provides the TWG and TACC daily intelligence briefings on significant, current developments potentially impacting AMC operations worldwide.

1.3.3.1. A team of briefers representing IN, USTRANSCOM/J2, AFOSI, SF, and TACC also provides the AMC/CC/CV Force Protection Briefings as required.

1.3.4. The TWG identifies airfield locations or facilities requiring force protection reviews, risk assessment, and/or briefing.

1.3.4.1. TWG action officers develop and coordinate risk assessments and develop force protection recommendations. Action officers also identify missions requiring Raven Team deployments.

1.3.4.2. TWG principals review and approve risk assessments and recommended force protection measures.

1.3.4.3. TWG passes force protection recommendations to appropriate command decision makers.

1.3.5. The TWG will follow the procedures outlined in **Attachment 3** for maintaining the Phoenix Raven required list.

1.3.6. The TWG will use the risk management tools in **Attachment 5 and Attachment 6** to determine force protection recommendations.

1.3.7. AMC's TWG program will comply with higher headquarters' guidance, policy, and doctrine.

1.3.7.1. AMC's Force Protection Board, which is a policy making forum that reviews high level force protection issues such as funding, training, and manpower, may task the TWG to staff FP-related issues.

1.4. Products:

1.4.1. TWG action officers produce written risk assessments and briefing products on airfields and specific geographic regions, as well as recommendations for force protection. TWG products include:

1.4.1.1. Secure Launch Country List: Unclassified document which identifies a country where the security situation is fluid and could deteriorate with little warning, creating such dangerous conditions that AMC aircraft scheduled to fly there would be at serious risk. A country is added to this list if it meets at least one of these criteria: CRITICAL or HIGH terrorism threat; chronic instability in the area of AMC operations; or a large US military presence or AMC footprint in a country that may provide an alluring target for anti-US elements.

1.4.1.2. Phoenix Raven Required Locations List: Unclassified document which identifies airfields where security is poor, and where additional threats, or the level of threat, indicate a need for specially trained Security Forces to provide dedicated aircraft security.

1.4.1.3. Man Portable Air Defense Vulnerability Risk Assessment (**Attachment 5**): Classified document which evaluates the portable SAM threat and the measures to mitigate against it.

1.4.1.4. Operation Risk Management Matrix (**Attachment 6**): Classified document which evaluates the overall terrorist, military, and criminal threats and the force protection mitigating measures. Forms primary baseline to determine "GO/NO GO" for individual missions.

1.4.1.5. TWG Recommendation Matrix: Classified comprehensive summary of all TWG force protection recommendations. Used for planning and executing AMC missions.

1.4.1.6. Risk Assessment (**Attachment 4**): Published classified analysis that details terrorist, military, criminal, medical, and IW threats and force protection recommendations at Secure Launch locations where AMC operates. Force protection recommendations could include, but are not limited to, the following:

1.4.1.6.1. Mission: Go/No go (if threat or risk is too high).

1.4.1.6.2. Employ aircraft defensive systems.

1.4.1.6.3. Vary arrival and departure times.

1.4.1.6.4. Restrict airfield operations to daylight or darkness hours only.

1.4.1.6.5. No RON.

1.4.1.6.6. Restrict MOG.

1.4.1.6.7. Deploy Raven Teams.

1.4.1.6.8. Enhance airfield security.

1.4.1.6.9. Stay on base.

1.4.1.6.10. Modified force protection recommendations for AMC-contracted commercial carriers.

1.4.2. The Force Protection Briefings cover the following areas:

1.4.2.1. Threat Information (OPR: AFOSI/IN/J2/AIA Det 4).

1.4.2.2. Operational Information (OPR: TACC).

1.4.2.3. Security Environment (airfield, billeting, etc.) (OPR: AFOSI Region 3/AMC/SF).

1.4.2.4. Force Protection Recommendations (OPR: TWG).

1.4.3. TWG products, e.g., risk assessments and briefings, are available to the TACC, SF, and AFOSI classified automated systems. These products are also sent electronically to AMC units at home station and are available on INTELINK-S.

1.4.3.1. AMC/INO disseminates specific intelligence updates and force protection information for AMC-contracted commercial carrier missions directly to the contracted commercial carrier's security manager or cleared mobilization representative as requested or as the threat dictates. Additional updates include:

1.4.3.2. Briefing updates to the aircrew via STU-III or in-person if an intelligence analyst is in place at an en route location.

1.4.3.3. Ensuring updates are provided to aircrews during a contingency at designated Senior Lodger locations, if activated, as designated by AMC/DOF or through the carriers' flight dispatch.

1.4.4. Aircrew debriefing, MISREPS, and Phoenix Raven Team post-mission reports provide feedback to the TWG on security risks to missions and force protection issues.

1.4.5. When required, the TWG provides written force protection inputs for HQ AMC Operations Orders during contingencies.

1.4.6. When required, the TWG also provides written force protection inputs for TACC CONOPS during CJCS exercises and contingencies.

Chapter 2

HEADQUARTERS AMC RESPONSIBILITIES

2.1. Director of Intelligence-(IN):

2.1.1. Serves as AMC's OPR and Chair for the TWG process.

2.1.2. AMC/IN is the focal point for all intelligence analysis, planning, direction, exploitation, production, and dissemination of intelligence to support the TWG processes.

2.1.3. Provides senior TACC controllers immediate analysis on critical information potentially impacting on-going AMC missions.

2.1.4. Provides current imagery, maps, and other current intelligence products.

2.1.5. Serves as facilitator for National Intelligence Agency representatives for the TWG.

2.1.6. Provides editing and production assets required to construct risk assessment briefings and products.

2.1.7. Provides the TWG with a meeting room (INCR) and all associated graphics support and coordination to ensure effective meetings.

2.1.8. Provides situational awareness briefings to the TWG in the form of daily current intelligence briefings.

2.1.9. Provides daily input to the TACC/XOZ on potential conflicts concerning AMC/CC/CV guidance on secure launch report (e.g., MOG/Raven Teams/FP measures).

2.1.10. Monitors the secure launch report to identify airfields requiring updated risk assessments, imagery, database, maps to ensure adequate force protection measures are in place prior to mission execution.

2.1.11. Places select TWG products on-line via INTELINK-S to ensure widest dissemination to active duty, guard and reserve AMC units.

2.1.12. Ensures all TALCES, AMEs, and TTFs have adequate force protection information and guidance prior to deployment of forces.

2.1.13. Identifies risk assessments in-progress and current priorities to the TWG on a weekly basis to allow TACC senior controllers to make adjustments as required.

2.1.14. Represents TWG in daily TACC Operations Review and validates force protection recommendations for the following day's scheduled Secure Launch and Raven required missions.

2.1.15. Produces a monthly Secure Launch Country List and threat matrix, utlilized by the TACC/XOC in accomplishing secure launch procedures.

2.1.16. Coordinates, produces, and disseminates weekly on-call list to ensure representatives of the TWG are available to TACC senior controllers (XOZ) at all times (e.g., after duty hours and weekends).

2.1.17. Provides military threat information from foreign countries to deployed AMC assets for all risk assessments.

2.1.18. Action officers participate, as required, in cross-functional team Force Protection briefings for AMC/CC/CV and senior staff.

2.2. Director of Security Forces-(SF):

2.2.1. Assesses adequacy of supported command force protection and security policies to provide adequate protection for AMC resources.

2.2.1.1. Assesses adequacy of force protection and security of AMC missions in countries listed on the Secure Launch Country List.

2.2.2. Ensures force protection initiative guidance is included in applicable security force directives.

2.2.3. Develops force protection and personnel protection guidance for inclusion in TWG risk assessments.

2.2.4. Ensures Raven Team taskings are forwarded to the appropriate TACC planners for inclusion in the GDSS.

2.2.5. Provides TWG action officers Raven Team post-mission reports.

2.2.6. Action officers participate, as required, in cross-functional Force Protection team briefings for AMC/CC/CV and senior staff.

2.2.7. Develops, maintains and disseminates Phoenix Raven required list.

2.3. Tanker Airlift Control Center (TACC)-(OPR: TACC/XOZ):

2.3.1. TACC/XOZ/XOC ensure TACC command and control issues related to TWG processes and force protection issues are adequately addressed in daily TWG meetings.

2.3.1.1. Participate as TACC/CC representatives to the TWG.

2.3.1.2. Provide the TWG current mission schedules and monitor on-going AMC missions.

2.3.1.3. Engage other TACC offices and processes required to facilitate TWG issues and taskings. Provide insight regarding TACC internal processes and players affecting or affected by TWG decisions and products.

2.3.1.4. Contact on-call TWG representatives during non-duty hours via TWG weekly on-call list (disseminated every Friday by 1730 hours).

2.3.2. TACC/XOP identifies CJCS exercise and contingency requirements to the TWG to include mission support force deployments, airlift flow, level of play, and any other unique requirements.

2.3.2.1. Provides CJCS exercises and contingency operational information for TWG Force Protection Briefings.

2.3.2.2. Provides a monthly projection for CJCS exercises and contingencies requiring TWG assessments and recommendations.

2.3.3. TACC/XOC/XOP action officers participate, as required, in cross-functional Force Protection team discussions and briefings for AMC/CC/CV and senior staff.

2.3.4. TACC/RF serves as advisors to the TWG on AMC-tasked Air Force Reserve and Air National Guard units and personnel.

2.4. AFOSI Region 3:

2.4.1. The primary mission of AFOSI Region 3 is to provide criminal investigative and counterintelligence support within AMC and Air Force Special Operations Command (AFSOC). As a member of the TWG, AFOSI Region 3/Office of Force Protection (FP) will advise the TWG on antiterrorism and counterintelligence issues (collection, investigation, or counterespionage-related matters).

2.4.2. Provides the TWG the latest threat information available on terrorism, crime, and foreign intelligence.

2.4.3. Action officers participate, as required, in cross-functional Force Protection team briefings for AMC/CC/CV and senior staff.

2.5. USTRANSCOM/J2:

2.5.1. The USTRANSCOM Joint Intelligence Center (JIC) performs a 24-hour Indications and Warning function for HQ AMC. During non-duty hours, the JIC notifies AMC Intelligence staff and TACC seniors of significant threats or changing world events affecting planned or on-going air mobility operations.

2.5.2. Serves as the conduit for collection requirement validation and RFI submission processes.

2.5.3. Provides current intelligence briefings during crisis or for special topics, as required.

2.5.4. Serves as the liaison between AMC and theater commands to ensure TWG threat recommendations are consistent with the theater recommendations.

2.5.5. Actively participates in the AMC TWG process; J2 action officer serves as the TWG recorder for daily meeting minutes.

2.5.6. Coordinates with AMC/IN on all TWG intelligence briefings and risk assessments.

2.6. USTRANSCOM Counterintelligence Support Office (CISO):

2.6.1. Provides Counterintelligence (CI) support for AMC operations by coordinating with service CI headquarters, the Joint Counterintelligence Support Branch (DIA), and the CI elements of the other unified commands.

2.7. Director of Central Intelligence Representative (DCI Rep):

2.7.1. Serves as the single point of contact for the TWG to the Central Intelligence Agency for intelligence and force protection issues.

2.7.2. Advises the TWG on activities involving CIA clandestine HUMINT intelligence, joint CIA/military operations, and provides the full range of CIA all-source analytical products and services to assist TWG force protection decisions and recommendations.

2.7.3. Provides DCI Counterterrorism Center analysis and comments on TWG risk assessments.

2.7.4. Provides inputs to the TWG on CIA intelligence collection capabilities and CIA all-source substantive intelligence analysis on matters of importance to TWG force protection decisions.

2.7.5. Responds in a timely fashion to intelligence information requests from the TWG.

2.7.6. Provides comments from CIA clandestine HUMINT collectors on TWG assessments.

2.7.7. Provides CIA Headquarters and field units with the Secure Launch Lists and Force Protection Essential Elements of Information (**Attachment 2**).

2.7.8. Provides tailored CIA analytical studies to support TWG decisions and recommendations.

2.8. National Security Agency Representative (NSA Rep):

2.8.1. Serves as the single point of contact for the TWG to the National Security Agency for intelligence and force protection issues.

2.8.2. Ensures all available NSA/Central Security Service (CSS) assets are used to efficiently meet the requirements of the TWG. Includes maintaining a Cryptologic Support Group (CSG TRANSCOM) at Joint Intelligence Center USTRANSCOM (JICTRANS) conducting continuous 24-hour SIGINT operations.

2.8.3. Advises and assists the TWG on issues to the exploitation, procurement, use and limitations of SIGINT in conducting operations in secure launch countries.

2.8.4. Advises and assists the TWG on issues relating to INFOSEC, OPSEC, and information operations.

2.8.5. Assists TWG in identifying intelligence requirements or gaps that could be resolved, in part or completely, through SIGINT operations. Assists in drafting requests for information (RFI) and time sensitive requirements (TSR) to fulfill requirements as needed.

2.8.6. Coordinates TWG requirements levied on the United States SIGINT System (USSS) and ensures appropriate NSA/CSS offices are cognizant of the needs. Provides AMC operational data such as the Secure Launch List to the USSS to aid in conducting operations.

2.8.7. Responds to TWG requests for SIGINT data either through local capabilities or through access to the USSS and ensures timely distribution of relevant SIGINT products.

2.8.8. Coordinates arrangements for en route flight following and threat advisories for aircraft transiting or terminating in areas suspected to be hostile to US military activities.

2.8.9. Arranges for rapidly deploying special intelligence collection activities in situations where limited SIGINT collection exists and conditions require more thorough intelligence coverage.

2.8.10. Assists in developing and coordinating intelligence positions, assessments, and recommendations on placing countries on the Secure Launch List, assessing threats at operating locations in these countries, and resolving other issues affecting air mobility operations.

2.9. Defense Intelligence Agency Representative (DIA Rep):

2.9.1. Serves as the single point of contact for the TWG to the Defense Intelligence Agency for intelligence and force protection issues.

2.9.2. Provides tailored, finished intelligence support to the TWG.

2.9.3. Coordinates and ensures DIA terrorism analysis and assessments are made available to the TWG.

2.9.4. Supports the TWG by ensuring that both RFIs and collection requirements generated by the TWG are given the proper visibility within DIA.

2.9.5. In concert with the USTRANSCOM Collection Management Office as appropriate, DIA will coordinate HUMINT collection with DHS Headquarters and the Defense Attaché Offices (DAO).

2.9.6. As required, communicates directly with DAOs to support TWG actions of an urgent or crisis nature.

2.9.7. Advises the TWG on Defense Human Intelligence (HUMINT) Service (DHS) collection activities as appropriate.

2.9.8. Provides DIA and the DAOs with the monthly Secure Launch Country List, as well as updates on secure launch missions.

2.9.9. Coordinates DIA and DAO input of TWG risk assessments, airfield surveys, and the general security situation in various countries using the Force Protection Essential Elements of Information (**Attachment 2**).

2.10. Counterintelligence Support-Air Force Office of Special Investigations (AFOSI): AFOSI is the agency within the USAF chartered and authorized to conduct counterintelligence activities in support of Air Force commanders worldwide. AFOSI Region 3, supports the TWG in both offensive and defensive roles.

2.10.1. The offensive role includes the following:

2.10.2. Counterespionage Operations. Operations to detect or neutralize the activities of foreign intelligence services directed at the USAF.

2.10.2.1. The defensive role includes the following:

2.10.2.2. Counterintelligence Collections. Collections focused on the timely and accurate production and dissemination of threat information relating to terrorists, foreign intelligence services, and criminal elements.

2.10.2.3. Counterintelligence Investigations. Investigations conducted to detect and neutralize planned and ongoing foreign intelligence. terrorist, or subversive activities targeting USAF personnel, resources, and information.

2.10.2.4. Intrusion Investigation and Analysis. Investigations conducted by computer crime investigators and analysts on intrusions into USAF computer systems.

2.11. Director of Operations (DO):

2.11.1. HQ AMC/DOK participates in the TWG as the representatives for the Director of Operations.

2.11.2. The DO representative will ensure operations issues related to TWG processes and force protection are addressed in daily TWG meetings.

2.11.3. Engages other DO offices as required to facilitate TWG issues and taskings. Provides insight regarding DO internal processes and organizations affecting or affected by TWG decisions/products.

2.11.4. Action officers assigned to DO will participate as required in cross-functional Force Protection team briefings for AMC Staff.

2.11.5.Will develop and maintain a tool to assess MANPAD vulnerability. This tool is the matrix at **Attachment 6.**

2.12. National Reconnaissance Office Representative (NRO Rep):

2.12.1. Optimizes all available NRO assets supporting TWG requirements. Additionally:

2.12.1.1. Advises/assists the TWG and National Agency Representatives.

2.12.1.2. Provides formal/informal training/education.

2.12.2. Serves as the TWG advisor regarding NRO Systems capabilities and limitations issues.

2.12.3. Develops and coordinates assessments and recommendations concerning National Systems support and future developments affecting TWG requirements.

2.13. Air Intelligence Agency (AIA)-Det 4:

2.13.1. Under the direction of AMC/IN, AIA (Det 4) provides the TWG with Information Operations (IO) threat expertise to improve situational awareness and facilitate courses of action.

2.13.2. Threat expertise will focus on adversary IO background, capabilities, and intentions as they could affect AMC missions.

2.13.3. The TWG will use this information to assess the IO threat to AMC missions and recommend courses of action to AMC/CV.

2.13.4. Provides OPSEC policy guidance and oversight to the TWG to protect friendly operations information from hostile intelligence sources when such sources are identified and potentially threatened AMC operations.

2.13.5. Provides AIA Reachback support to TWG.

Chapter 3

WING, DIRECT REPORTING UNIT (DRU), AND GEOGRAPHICALLY SEPARATED UNIT (GSU) LEVEL RESPONSIBILITIES

3.1. Requirements . This chapter contains minimum requirements for establishing and maintaining the Threat Working Group (TWG) program at the unit level.

3.1.1. Each Wing, DRU, and GSU should convene a TWG to review force protection issues relating to assigned AMC missions. The unit commander may also convene a TWG as deemed necessary based on the local security situation and directives.

3.1.2. The TWG membership, as a minimum. should include representatives from operations, intelligence, AFOSI, and security.

3.1.2.1. Coordinate with supporting AFOSI and Security Forces when membership is not available.

3.2. Responsibilities:

3.2.1. Review appropriate HQ AMC TWG's risk assessments and force protection recommendations.

3.2.2. Evaluate local threat situation as appropriate.

3.2.3. Develop and document procedures to implement HQ AMC TWG Force Protection recommendations.

3.2.4. Produce timely MISREPS in accordance with AMCI 14-102, *Debriefing and Reporting*, to assist local and HQ level TWGs better assess in-place force protection measures and determine the need for additional force protection requirements and actions.

3.2.5. Request/coordinate force protection issues with HQ AMC TWG members.

ROGER D. MAHER, Colonel, USAF
Director of Intelligence

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*

Joint Pub 3-07-2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*

USTCH 31-2, *Security Awareness Guide to Combating Terrorism*

AFPD 10-11, *Operations Security*

AFPD 31-1, *Physical Security*

AFPD 31-4, *Information Security*

AFPD 71-1, *Criminal Investigations and Counterintelligence*

AFI 10-1101, *Operations Security*

AFI 14-105, *Unit Intelligence Mission, and Responsibilities*

AFI 31-101, *Volume 2, The Air Force Physical Security Program*

AFJI 31-102, *Physical Security*

AF131-207, *Arming and Use of Force by Air Force Personnel*

AFI 31-209, *Air Force Resource Protection Program*

AFI 31-210, *The Air Force Antiterrorism (AT) Program*

AFI 31-401, *Managing the Information Security Program*

AFI 31-501, *Personnel Security Management Program*

AFI 31-601, *Industrial Security Program Management*

AFI 31-702, *System Security Engineering*

AFI 31-703, *Product Security*

AFI 71-101, *Volume 1, Criminal Investigations*

AFOSI Instruction 71-104, *Volume 1, Counterintelligence and Security Services*

AMCI 14-102, *Debriefing and Reporting (Atch 5 EEI List)*

AMCPAM 14-104, *Intelligence Cookbook*

AMCI 31-104, *Phoenix Raven Program*

AMCR 55-37, *Air Operations Security*

Abbreviations and Acronyms

AAFIF—Automated Air Facility Intelligence File

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFSOC—Air Force Special Operations Command

AMC—Air Mobility Command

AMCI—Air Mobility Command Instruction

AME—Air Mobility Element

AMMP—Air Mobility Master Plan

AOR—Area of Responsibility

AT—Antiterrorism

CI—Counterintelligence

CIA—Central Intelligence Agency

CJCS—Chairman, Joint Chiefs of Staff

CMW—Compartmented Mode Workstations

COMSEC—Communications Security

CONOPS—Concept of Operations

CSG—Cryptologic Support Group

CSS—Central Security Service

CT—Counterterrorism

DAO—Defense Attaché Office

DCI—Director of Central Intelligence

DHS—Defense HUMINT Services

DIA—Defense Intelligence Agency

DoD—Department of Defense

DoDD—Department of Defense Directive

DRU—Direct Reporting Unit

DS—Defensive Systems

EEI—Essential Elements of Information

FAA—Federal Aviation Administration

FP—Force Protection

GDSS—Global Decision Support System

HUMINT—Human Resource Intelligence

I&W—Indications and Warning

IIR—Intelligence Information Report

IMINT—Imagery Intelligence

IN—Chief of Intelligence (Air Force, MAJCOM, Wing, Group)

INCR—Intelligence Conference Room

INTELINK-S—Intelligence Link (a secure "internet" for classified information)

INFOSEC—Information Security

IO—Information Operations

IW—Information Warfare

J2—Director of Intelligence

JCS—Joint Chiefs of Staff

JIC—Joint Intelligence Center

JWICS—Joint Worldwide Intelligence Communications System

MANPADS—Man Portable Air Defense System

MC&G—Mapping, Charting, and Geodesy

MISREPS—Mission Reports

MOG—Maximum on Ground

NIMA—National Imagery and Mapping Agency

NPIC—National Photographic Interpretation Center

NRO—National Reconnaissance Office

NSA—National Security Agency

OPLAN—Operations Plan

OPORD—Operations Order

OPR—Office of Primary Responsibility

OPSEC—Operations Security

RFI—Request for Information

RON—Remain Over Night

RSO—Regional Security Officer

SCI—Sensitive Compartmented Information

SIGINT—Signals Intelligence

SITREP—Situation Report

SF—Security Force

TACC—Tanker Airlift Control Center

TALCE—Tanker Airlift Control Element

TSR—Time Sensitive Requirement

TTF—Tanker Task Force

TWG—Threat Working Group

USSS—United States SIGINT System

VTC—Video Teleconference

Terms

Antiterrorism—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

Counterintelligence—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

Counterterrorism—Offensive measures taken to prevent, deter and respond to terrorism.

Information—Information is defined as data and the instruction required to give that data meaning.

Information Warfare (IW)—IW is action taken to deny, exploit, corrupt, or destroy an adversary's information, information systems, and information operations, while protecting friendly forces against similar actions.

Operations Security (OPSEC)—A process identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to identify those actions that can be observed by adversary intelligence systems; determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together critical information in time to be useful to adversaries; or select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

PHOENIX RAVEN TEAM—Two to four person "Fly-Away" Security Team tasked with providing close-in security for AMC aircraft at OCONUS areas where the local security has been assessed as inadequate or the security situation is not fully known.

Attachment 2

AIR MOBILITY COMMAND'SFORCE PROTECTIONESSENTIAL ELEMENTS OF INFORMATION

1. When conducting an airfield survey, use the following questions to complete your report. Your report should be in paragraph format, explaining the questions in as much detail as possible. Those items identified by an asterisk (*) are considered critical information to be included in your report.

2. Airfield Name/Location:____________________ ICAO____________ Date: ________

2.1. FENCING/WALLS

Is the airfield perimeter completely fenced or walled (type, height, condition, gaps, holes, etc)?

Is the flightline/ramp fenced? Describe (type, height, condition, gaps, holes, etc)?

Are there clear zones on each side of the fence/wall?

Is the airfield perimeter or flightline area posted "No Trespassing" or "No Admittance"?

2.2. OTHER PHYSICAL BARRIERS

List different types, locations, and numbers of barriers used on the perimeter, and on/near the flightline/ramp.

Is the airfield or aircraft parking areas under close circuit TV (CCTV)?

2.3. SECURITY FORCE LEVEL

How many guards are typically on duty during the day and night?

Are these guards host military units? Police or security police? Or contract personnel?

To what extent and for how long can this force be augmented by in-place/nearby personnel?

Shift duration and shift change procedures/times.

What local customs might result in decreased security (e.g. national holidays, traditional daily rest periods, etc)?

2.4. SECURITY PERSONNEL

Are personnel well trained and professional (does this vary by position; are the supervisory personnel better trained or more motivated)?

What factors make individual members or groups susceptible to blackmail/bribery (e.g. low pay, irregular pay, mistreatment by senior leadership etc)

What is the predominant language/dialect spoken by security forces (also indicate what percentage speak English, if applicable)

To what degree are they willing to work with U.S./Allied personnel?

Are security forces willing/able to provide increased security for U.S./Allied missions?

If so, how are such arrangements made? Through DAO office?

2.5. PATROLS

Is the perimeter and/or flightline controlled by armed guards?

Frequency and regularity of patrols. (Are the patrols conducted on a predictable schedule or are they conducted randomly by the airport security force? If not on a regular schedule, is the variance purposeful (i.e. a security measure)?

Is patrol made on foot, animals, or vehicles?

How many people are on each patrol?

Do patrols use military working dogs (MWD)?

2.6. SECURITY EQUIPMENT

What types of weapons are carried by guards?

What additional weapons are available (what weapons can be used, if needed; what weapons are used on vehicles, at entry points, guard towers, etc)?

What forms of communications gear do the security personnel use?

2.7. WATCH TOWERS/FIXED GUARD POSITIONS

Number, location, and description (ground level guard shack, elevated tower, fixed fighting positions/bunkers, etc)

Number of guards at each location.

2.8. QUICK REACTION/COUNTERTERRORIST UNITS

Does such a force exist?

Is it on or near the airport?

What is its reaction time?

How large a force is it?

To what degree is responsibility delegated in crisis situations.

How is the forced trained and equipped?

Does it have higher morale that the regular guard force?

Has it successfully conducted operations in the past?

2.9. ENTRY CONTROL POINTS

Is entry controlled to the installation and flightline/ramp?

Number, location and description of ECPs at the perimeter and flightline/ramp areas.

Are gates locked if unmanned?

Number of guards at each entry point (military/civilian, airport police, day/night)

Are x-ray machines and /or metal detectors used at any of the entry points?

If entry is controlled, what form(s) of personal identification are required for individuals and vehicles?

Are private vehicles allowed?

If so, what method of registration is required?

Are all persons in a vehicle required to show identification?

What are visitor control procedures (i.e., procedures for visitor approval, identification of same)?

What are visitor escort procedures?

To what degree are vehicles, personnel and their possessions searched?

Do any of the above procedures vary at night (i.e., all personnel must show identification at night when entering the installation, etc)?

2.10. LIGHTING

Is entire boundary, flightline and parking ramp lighted at night?

Are additional fixed spotlights located at watchtowers/entry points?

Are mobile mounted/towable spotlights available?

2.11. PARKING

Are U.S. Government aircraft parked in special locations?

If so, are additional guards posted?

Is the area clearly marked as a restricted area?

Are U.S. personnel authorized to have weapons on the flightline/ramp?

Are weapons storage facilities available to transient crews?

3. BILLETING (use when AMC aircraft must remain over night at foreign airfields)

Does AMEMBASSY provide billeting in its compound?

If billeting is unavailable at the compound, does AMEMBAASSY/DAO maintain a list of hotels that meet minimum security requirements?

If AMEMBASSY maintains a standing list of recommended hotels, request the following information on each if available:

Basic description (design, height, towers, interior/exterior entrances, number of rooms)

General layout (parking areas, fencing, lighting, proximity to highways/major roads)

Number of elevators/stairways (internal/exterior), building entrances/exits, vehicle entrances/exits.

Are U.S. personnel billeted in the same areas of the hotel or are they separated?

How is the crew transported to and from the hotel?

Are metal detectors/x-ray machines used at hotel entrances?

Are security forces available to escort crews transiting to/from airport?

4. OFF INSTALLATION ROUTE SECURITY (use when AMC aircraft must remain over night at foreign airfields)

Distance from airport to hotel.

Number of different routes from airport to hotel.

Route description(s).

Choke points on route (to include excessive traffic lights, congestion)

Number of lanes each way.

One-way streets?
Number and location of safe houses (i.e., police stations) along route.

Does host nation regularly patrol these routes?

Any bridges, overpasses or tunnels along the route?

5. PERSONNEL THREAT

Are dissidents known to operate in the area of the airport?

Identify these groups by name with leaders if known.

Are dissidents known to possess stand-off weapons (SAMS, RPG, mortar, etc, (specific type and any known modification)

Are these groups known to possess communications monitoring equipment (identify type and capability if known)?

Are these groups known to have anti-U.S. sentiments?

What past incidents have occurred which targeting of U.S. personnel, equipment, facilities occurred?

Do hostile elements have any specific times/dates when they are historically active?

Do they have the support of the local populace?

6. PHYSICAL LOCATION

What natural/manmade obstacles are in the vicinity of the airport (e.g., power lines, tall buildings, etc)?

Identify areas surrounding flightline parking, which could be used by hostile elements to covertly surveil airport operations and to launch attacks?

How suitable is the surrounding terrain and vegetation for a standoff attack? Does this vary seasonally?

7. Please include maps or a sketch locating security information (aircraft parking areas, fencing, lighting, ECPs, etc.). Digital photos of all items are requested, if capability exists.

8. When complete, send your report to HQ AMC/SFGC, DSN FAX 576-8645, or send by E-mail to the OPR at ____________@hqamc.scott.af.mil Any questions can be addressed to HQ AMC/SFGC at DSN 576-2950.

Attachment 3

PHOENIX RAVEN REQUIRED LIST MAINTENANCE PROCESS

This attachment outlines the process for maintaining the PHOENIX RAVEN (PR) Required List (PRRL) within the Threat Working Group (TWG) and then passing this information to the TACC, CV, and other AMC decision-makers.

1. Coordination

a. SF will assume "process ownership" for updating the PRRL and coordinate with other TWG members to determine which locations should be PR-required.

b. Any member of the TWG may request evaluation of a location for potential inclusion on the PRRL.

2. Approval

a. Once SF, IN and AFOSI Region 3 reach agreement on a recommendation, the initiating TWG member will draft a point paper justifying the recommendation and present it to the TWG for approval.

3. Dissemination

a. Once approved, SF will distribute the point paper to appropriate organizations and ensure necessary Global Decision Support System (GDSS) fields are updated.

b. IN will ensure the PR location update is reflected in appropriate TWG products (TWG Recommendations Matrix, Risk Assessments, and PRRL) and disseminated the next day via INTELINK-S and hard-copy.

Attachment 4

SAMPLE
AMC THREAT WORKING GROUP (TWG)
AIRFIELD RISK ASSESSMENT
VALID AS OF XX XXX 99

SUBJECT: XXXXXX Airfield, XXX Country (ICAO) Risk Assessment (U)

LOCATION:

- (U) General Location: 8 mi. south of capital city.

-- (U) This section will give a general location for the airfield relative to a major city and may provide coordinates

TERRORIST THREAT: -*AOR*-

- (U) Terrorist threat to American interests in the XXX (country) is **HIGH**

-- (U) This section will describe capabilities, intent and history of terrorist groups to target or observe US citizens or assets within the country

-- (U) Provides information on modus operandi of the known terrorist groups within the country

-- (U) Gives details on any recent specific terrorist attacks on US citizens and assets

MILITARY THREAT: -*AMC/IN*-

- (U) The military threat to AMC air and ground operations is **LOW**

-- (U) This section will provide information on the history or intent of the host nation military or the regional militaries to target US or allied assets

-- (U) Provided details on any recent specific encounters between host nation/regional militaries with USAF assets

CRIMINAL THREAT: *-AFOSI-*

- (U) The criminal threat to AMC aircrew/personnel in Kuwait is **LOW**

-- (U) This section provides information on crimes that occur routinely within the country or region with special attention to the airfield and its vicinity

-- (U) Gives an idea of what serious crimes could occur in the region

-- (U) Discusses availability of weapons to criminal elements, problems stemming from drug trafficking, and similar issues

-- (U) Discusses measures US personnel should take to avoid becoming a victim of crime

-- (U) Advises on most secure billeting options available and route security concerns between the airport and billeting

FOREIGN INTELLIGENCE THREAT: *-AFOSI-*

- (U) There is no evidence country XXX’s intelligence services are actively targeting US assets

-- (U) This section will provide specifics on what intelligence services (host-nation and regional) are specifically targeting US personnel and what their priority is on collection that information

-- (U) Provides capability to collect information and modus operandi of collection practices

THREAT MITIGATING TACTICS: *-AMC/DO-*

- (U) The most important operational threat to MAC operations into XXX airfield is XXX. Take the following measures to mitigate that threat…

-- (U) This section will cover tactics recommended to counteract potential threats to AMC operations

INFORMATION OPERATIONS THREAT: *-AMC/IN-*

- (U) The most vital information operation threat to AMC assets is XXX

-- (U) This section will discuss specifics on host nation entities and others who have the capability or intent of using information operations to target US forces

-- (U) Covers any targeting of government computers, phone lines, monitoring of friendly mission-related information (OPSEC), psychological operations employed by the enemy, etc

MEDICAL THREAT: -A*MC/SG*-

- (U) The most pressing medical concern at XXX airfield is XXX

-- (U) As applicable, this section covers any medical concerns with endemic diseases and what actions US personnel should take to prevent those diseases

-- (U) Discusses sanitary conditions at the airfield/in the country and practices that should be taken to mitigate the speed of disease

-- (U) May cover climate concerns and what should be done to prevent hypothermia, dehydration, etc

-- (U) Covers host nation medical treatment facilities/capabilities and the location of US-run medical facilities within the country

AIRFIELD SECURITY: -*AMC/SF*-

- (U) The airfield security at airfield XXX is considered good

-- (U) This section will provide an overview of the security at and around XXX airfield

--- (U) Provides specifics on fencing, lighting, entry control points, line badge system, and security forces responsible for patrolling the airfield, including their effectiveness; in addition to other specifics on airfield security

TWG RECOMMENDATIONS: -*AMC/TWG*-

(U) Given adherence to security procedures and a LOW terrorism threat level, the probality of an attack on AMC assets at XXX Airfeild is LOW

(U) This section will cover specific actions that should be taken in response to the assessed threat in all of the above areas

Recommendations could be operational in nature or related to personal protection and could include any of the following:

- Use DS Equipment to the maximum extent possible
- Use armor
- Restrict the maximum on ground (MOG) limit
- Restrict operation hours to day or night only depending on the threat
- Do not remain over night (RON)
- Include Phoenix Raven teams for mission
- Vary arrival/departure times
- Carry chemical gear
- Billet on base
- Suggest personnel protection measures

DS EQUIPPED	**ARMOR**	**MOG OF ONE**	**DAYLIGHT OPS ONLY**	**NIGHT OPS ONLY**	**NO RON**	**RAVEN REQUIRED**
MEP*		**X@**			**X**	

*Maximum extent possible	**X** @: Deviation requires CV approval	**X**: Deviation requires TACC/CC approval

____________	____________	____________	____________	____________	____________
AMC/IN	USTC/J2	TACC/XOC	AMC/SF	AFOSI	AMC/DOK

1Lt Katrina J. Hebert/HQ AMC INOA/5180/kjk/27 Jan 99
CLASSIFIED BY: XXXXXX
DECLASSIFY ON: XX XXX XX

Attachment 5

AIRFIELD MANPAD THREAT ASSESSMENT

SAMPLEAirfield MANPAD Threat Assessment: ____________________					
Factors (OPR)	A	B	C	D	E
1. MANPAD Availability for Hostile Elements (IN/OSI)	MANPAD presence highly unlikely	Potential of MANPADs in the country	Specific reporting of MANPADs in country, source credibility undetermined	Specific reporting of MANPADs in country, credible source/ multiple sources	Confirmed evidence of MANPADs in the country
	0	5	10 14	15 20	25
2. Intent to Carry out MANPAD Attack (Actual MANPAD use warrants additional assessment) (IN/OSI)	No assessed intent to use MANPADs and negligible likelihood that MANPADs are possessed by opposition groups	No assessed intent to use MANPADs but ikelihood exists that MANPADs are possessed by opposition groups	Assessed intent to use MANPADs and slight likelihood that MANPADs are possessed by opposition groups	Assessed intent to use MANPADs and moderate likelihood that MANPADs are possessed by opposition groups	Assessed intent to use MANPADs and high likelihood that MANPADs are possessed by opposition groups
	0	5	11 20	21 40	50
STOP: If Total Score of Factors 1 and 2 is 20 or Less, NO DS Requirement; NO additional assessment is required					
3. Internal Security (IN/OSI)	Excellent Internal Security	Good Internal Security	Moderate Internal Security	Undetermined/poor Internal Security	Critical Internal Security
	-15	-10	0	10	15
4. Terrorist Threat (IN)	Negligible	Low	Medium	High	Critical
	0	5	15	25	35
5. Military Threat (IN)	Negligible	Low	Medium	High	Critical
	0	5	15	25	35

SAMPLEAirfield MANPAD Threat Assessment: ________________________					
Factors (OPR)	A	B	C	D	E
6. Government Stability/Regional Political Tensions (IN)	No open conflict or tangible intent to destabilize the government	No open conflict; Opposition group has destabilizing influences	Intermittent conflict in the region and/or government involved in occasional skirmishes with opposition group(s)	Open armed conflict in immediate region and/or gov't engaged in persistent conflict with opposition group(s)	Open armed conflict in the immediate region and/or government facing serious threats to survival.
	0	5	10	15	20
7. Security of MANPAD Footprint (SF/OSI)	MANPADS footprint closely monitored by US/Host Nation Military Personnel (open terrain)	MANPADS footprint closely monitored by Host Nation Military/Civilian police (open terrain)	MANPADS footprint closely monitored by US/Host Nation Military/Civilian police (rugged or urban terrain)	Daily random day and night patrols of MANPADS footprint by host nation military/civilian police (rugged or urban terrain)	No Exterior Security or Patrolling
	-25	-5	0	10	25
8. Mission (Frequency, predictability, profile) (TACC)	Low mission frequency, unpredictable, and low profile	Moderate mission frequency, unpredictable, and low profile (1 of 3)	Moderate mission frequency, unpredictable, and low profile (2 of 3)	Moderate mission frequency, unpredictable, and low profile (3 of 3)	High mission frequency, highly unpredictable, and high profile
	-10	0 4	5 15	16 25	30
0-70 points. No DS requirements.	71-110 points. Use DS to Max Extent Possible. No approval required to waive use of DS.	111-145 points. Use DS to Max Extent Possible. TACC/CC approval to waive requirement.	146+. All missions require use of DS. AMC/CC or AMC/CV approval to waive requirement.	Total for This Airfield (Max Possible Score: 235)	

SAMPLEAirfield MANPAD Threat Assessment: ________________________					
Factors (OPR)	A	B	C	D	E
Mitigating Factors	Ability to use blacked out operations, or terrain masking, or TAA/D (all 3 applicable)	Ability to use blacked out operations, or terrain masking, or TAA/D (any 2 of 3 applicable)	Ability to intermingle commenrcial and military aircraft at night (not used in conjunction with tactics)	Ability to use blacked out operations, or terrain masking, or TAA/D (any 1 of 3 applicable)	No mitigating factor
	-25	-15	-10	-5	0

Attachment 6

AMC THREAT WORKING GROUP OPERATIONAL RISK ASSESSMENT

If Mission Profile and MANPAD Vulnerability is High, Consideration of Additional Steps to Mitigate the Threat Should be Considered

ICAO:	**AMC THREAT WORKING GROUP** OPERATIONAL RISK ASSESSMENT	**RAVEN REQUIRED: YES / NO**

NAME/LOCATION OF AIRFIELD: **DATE ASSESSED:**

DATA SOURCE:

The criminal threat is:	Negligible: 0 Points	Low: 5 Points	Medium: 15 Points	High: 25 Points	Critical: 35 Points
The Terrorist Threat is:	Negligible: 0 points	Low: 10 points	Medium: 20 points	High: 30 points	Critical: 35 points
The Military Threat is:	Negligible: 0 Points	Low: 0 Points	Medium: 20 Points	High: 60 Points	Critical : 95 Points
FACTORS	0 POINTS	5 POINTS	10 POINTS	15 POINTS	20 POINTS
Installation/airport security services are:	provided by US military	Host nation or contract security, reliability is not in question	host nation or contract security, reliability is unknown	Host nation or contract security, reliability is in question	No organized security available
Host security forces control entry:	Via a manned installation entry point and a credential check for flightline access	to the flightline only	to the installation/ airport only	to neither the flightline or installation/ airport	
There is perimeter fencing or barriers around:	the flightline & installation/ airfield perimeter	the flightline only	to the installation/ airfield perimeter only	none available	

Security forces will _____ security incidents involving the aircraft.	provide US area patrol and 5 minute armed response (AFI 31-101 standards)	provide armed response to	provide unarmed response to	notify the aircraft commander or civilian authorities of	
The aircraft will be parked:	in a US military aircraft only parking area	separate from host military and civilian aircraft	among other host military aircraft only	among other civilian aircraft	
Illumination will:	be area and perimeter lighting	be area lighting only	be perimeter lighting only	No lighting available	
Security measures at billeting are: (Consider if RON)	on base or within US government facility	surveillance of entry/exit with armed security	security personnel (armed or unarmed) on duty 24 hours	non-existent	
Routes of travel between the airfield and billeting are: (Consider if RON)	multiple routes with negligible vulnerabilities	multiple routes with contract drivers or escort	multiple routes with some vulnerabilities without assigned driver or escort	single/multiple route with vulnerabilities without assigned driver or escort	
GRAND TOTAL:					

5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	125	130	135 +

MAINTAIN AWARENESS CONSIDER MITIGATING MEASURES CONSIDER
CANCELLING MISSION

(135+ - STRONGLY CONSIDER CANCELLING MISSION)